REMARKS

The Examiner has rejected Claims 1, 10, 20, 26, 33, 39, 46, 51, 57, 60, 64, and 67 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. More specifically, the Examiner asserts that the claim limitation of "a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames" is self-contradicting. Applicant respectfully asserts that the first cited limitation, "a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key," is to be read as storing at least one of *the encryption cryptographic key and the decryption cryptographic key*. In other words, the claims require a removable storage medium storing either the *encryption* cryptographic key, the *decryption* cryptographic key, or both, but does not require storage of more than one of each. As a result, a removable storage medium will store no more than one *encryption* cryptographic key, which is consistent with the second cited limitation.

The Examiner has also rejected Claims 1, 3, 5-7, 10, 12, 14-16, 19-20, 22-24, 26, 28-30, 32-33, 35-37, 39, 42-43, 45-46, 48, 51, 53, 56-58, 60-61, 63-65, 67 and 70 under 35 U.S.C. 103(a) as being unpatentable over Brothers (U.S. Patent No. 5,799,083) in view of Barton (U.S. Patent No. 5,912,972) and in view of Tsuria (U.S. Patent No. 6,178.242). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to independent Claim 1 et al., the Examiner's response to applicant's arguments relies on the following excerpts from the Barton and Brothers references to make a prior art showing of applicant's claimed "verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding

decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash".

> "...authentication of a digital block and for carrying additional authentication information provided by the user, i.e. meta-data, in a secure and reliable fashion. To embed authentication data into a digital block, a digital signature is formed that is a reduced representation of the digital block. The signature and additional information supplied by the user are embedded into the digital block by replacing predetermined bits within the block. Encryption can be used to enhance..." (Barton: Col. 4, lines 20-27)
>
> "Uniqueness: The block size must be chosen to match the digital signature technique, or vice-versa. The goal is to achieve as unique a signature as possible, within the bounds of cost and efficiency. For instance, a 16-bit checksum is appropriate for very small blocks (e.g. a few tens of bytes) and is also very quickly calculated, while a Fourier transform is appropriate for very large blocks, but takes a great amount of time to calculate." (Barton: Col. 6, lines 37-44)
>
> "4. Encrypt the embedded bit string using any useful encryption technique (16), such as the DES encryption standard promoted by the National Institute of Standards, which uses a private-key algorithm to encrypt the data. Greater security may be obtained using the RSA public-key encryption technique, a patented method in which different keys are used for encryption and decryption (see U.S. Pat. No. 4,405,829). If desired after encryption, append to the string to be embedded a bit string indicating the encryption technique employed. For more secure applications, this last step should not be done." (Barton: Col. 7, lines 16-26)
>
> "...an additional measure for authentication. Because the encrypted video frames are stored in memory 74 at the..." (Brothers: Col. 10, lines 48-49)

The above references teach the formation of a digital signature to embed authentication data into a digital block, the matching of block size to a digital signature technique, the encryption of a bit string using a useful encryption technique, and the existence of encrypted video frames. Nowhere in such excerpts is applicant's "verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash" (emphasis added), as claimed.

Additionally, with respect to the independent claims, the Examiner's response to applicant's arguments relies on the following excerpts from the Brothers and Tsuria references to make a prior art showing of applicant's claimed "validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames" (see this or similar, but not necessarily identical language in each of the independent claims).

> "...produced upon identification of a user of the apparatus of FIG. 1 by any method well known in the art, such as by provision of a personal identification number (PIN)." (Tsuria: Col. 8, lines 63-65)
>
> "...Storing the encrypted samples not only preserves a verifiable portion of the recorded event as a backup against loss or destruction of the digital tape 38, but it also contributes an additional measure for authentication. Because the encrypted video frames are stored in memory 74 at the..." (Brothers: Col. 10, lines 45-49)

The above excerpts teach the production of a TECM key upon identification of a user, the storing of encrypted video frames in memory, and the storage of encrypted samples. On the other hand, applicant's claims require a "validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames" (emphasis added), as claimed. The Tsuria reference merely describes a TECM key, where such TECM key is utilized to encode a TECM. Nowhere in the cited language is a decryption cryptographic key validated against user-provided credentials prior to decrypting the encrypted frames, as claimed.

Furthermore, with respect to the independent claims, the Examiner's response to applicant's arguments relies on the following excerpt from the Tsuria reference to make a prior art showing of applicant's claimed "set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key" (see this or similar, but not necessarily identical language in each of the independent claims).

"The system of FIG. 1 also comprises a removable security element, such as a smart card 120, in removable operative attachment with the IRD 110. The smart card 120 is typically suitably programmed, as is well-known in the art, to provide control words (CWs) for descrambling of a scrambled broadcast digital data stream by the IRD 110. Methods for programming and utilizing smart cards such as the smart card 120 to produce CWs are well-known in the art and are described, for example, in U.S. Pat. No. 5,282,249 to Cohen et al. and U.S. Pat. No. 5,481,609 to Cohen et al., referred to above, with suitable modifications, as are well-known in the art and described above, particularly in the MPEG-2 standard, for operating on digital rather than on analog data." (Tsuria: Col. 6, line 63- Col. 7, line 8)

Applicant respectfully reasserts that such excerpt only teaches a smart card that is "programmed...to provide control words (CWs) for descrambling of a scrambled broadcast digital data stream." Clearly, a smart card that is capable of providing control words, as in Tsuria, does not meet any sort of "set of cryptographic instructions....employing at least one of the encryption cryptographic key and the decryption cryptographic key," as claimed by applicant (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, as follows:

"wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player" (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully asserts that the above amendments made to the independent claims require a "physical boundary separating the transportable storage medium from a player" (emphasis added) and a "physical boundary separating the transportable storage medium from the player" (emphasis added). Further, applicant claims require that "only encrypted video content ... [and] ... only the signed video content ... passes the ... physical boundary" (emphasis added). A notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

It is noted that the Examiner has still not responded to applicant's previously submitted arguments with respect to the dependent claims. Such arguments are reiterated below for proper consideration.

With respect to the subject matter of dependent claim 3 et al., "an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key" (now at least substantially incorporated into each of the independent claims), the Examiner has simply dismissed the same under Official Notice. Applicant notes that upon careful inspection of the cited references, none of the prior art teaches the use of a

private key corresponding to the *encryption* cryptographic key and a *public* key corresponding to the *decryption* cryptographic key. Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

"If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

With respect to the subject matter of former Claims 5 and 6 et al. (now at least substantially incorporated into each of the independent claims), the Examiner has relied on the following excerpts from the Barton reference to make a prior art showing of applicant's claimed "asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair" (see this or similar, but not necessarily identical language in each of the independent claims).

> "...which uses a private-key algorithm to encrypt the data. Greater security may be obtained using the RSA public-key encryption technique, a patented method in which different keys are used for encryption and decryption (see U.S. Pat. No. 4,405,829). If desired after encryption, append to the string to be embedded a bit string indicating the encryption technique employed. For more secure applications, this last step should not be done. (Col. 7, lines 19-26)

The Barton reference teaches the use of a private-key algorithm and a RSA public-key encryption technique. However, applicant limits the asymmetric cryptographic key pair to comprise at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair. Not only does the Barton reference fail to do this, but also all references cited by examiner fail to mention either the TwoFish or Diffie-Hellman-compatible encryption algorithms or key pairs. As a result, applicant's claims are unique.

Again, Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

All of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P383/01.023.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100